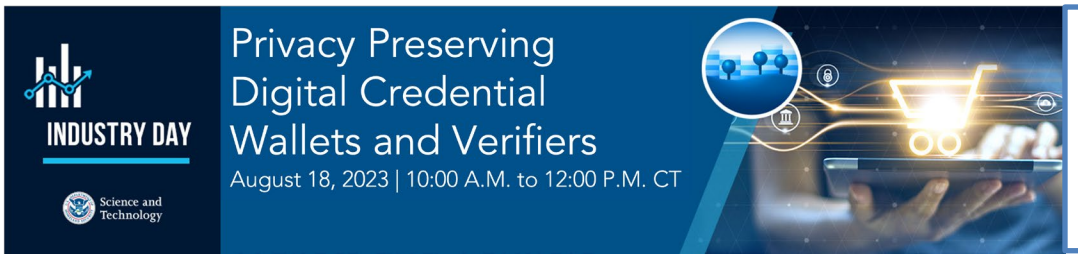
Homeland Security

DHS S&T Silicon Valley Innovation Program (SVIP)

PRIVACY PRESERVING DIGITAL CREDENTIAL WALLETS & VERIFIERS

Other Transaction Solicitation Call
70RSAT23R00000034



Application Forms @ SAM.gov

Application Deadline
15 September 2023, 12:00 PM PT

https://www.dhs.gov/science-and-technology/svip
DHS-Silicon-Valley@hq.dhs.gov

1. Introduction

This Other Transaction Solicitation (OTS) Call 70RSAT23R00000034 is being issued against the Department of Homeland Security (DHS) Science & Technology Directorate (S&T) Silicon Valley Innovation Program (SVIP) 5-Year Innovation OTS (70RSAT21R00000006). All terms and conditions of the DHS S&T SVIP 5-Year Innovation OTS (70RSAT21R00000006) remain incorporated into this Call unless otherwise noted herein.

The U.S. DHS is committed to using cutting-edge technologies and scientific talent in its quest to make America safer while safeguarding privacy, civil rights, and civil liberties. The DHS S&T SVIP, on behalf of DHS Operational Components, invests in startup companies with viable technologies suitable for rapid prototyping projects from across the nation and around the world to adapt, develop and harness cutting-edge capabilities that are commercially sustainable while simultaneously meeting the needs of DHS Operational Components and Programs.

1.1. DHS Operational Need

DHS Operational Components are globally authoritative issuers and verifiers of identifiers, licenses, entitlements, attestations, and certifications, a.k.a. credentials, for a variety of purposes including immigration, residency status, employment eligibility, travel, training, education, affiliation, benefits delivery, organizational identity, and supply chain security.

DHS Operational Components, particularly U.S. Citizenship and Immigration Services (USCIS) and U.S. Customs and Border Protection (CBP), with the support of the DHS Privacy Office (PRIV) have been early adopters and champions in seeking to implement privacy preserving capabilities into the digital issuance and verification of these various credential types using World Wide Web Consortium (W3C) Verifiable Credential Data Model (VCDM)[1] and W3C Decentralized Identifiers (DIDs)[2], which are global standards developed openly by a diverse technical community at the W3C that are patent free, royalty free and free to use by anyone.

This SVIP Call seeks privacy preserving technical capabilities that directly support and integrate with the three-party digital identity model (issuer, holder, verifier) enabled by W3C VCDM and W3C DIDs, that could serve the mission needs of DHS Operational Components and Offices including:

- *U.S. Citizenship and Immigration Services (USCIS)*
- *U.S. Customs and Border Protection (CBP)*
- *DHS Privacy Office (PRIV)*

1.2. Support the National Strategy to Advance Privacy-Preserving Data Sharing and Analytics

The "National Strategy to Advance Privacy-Preserving Data Sharing and Analytics (PPDSA)"[3] articulates how "Privacy-preserving data sharing and analytics technologies help advance the well-being and prosperity of individuals and society and promote science and innovation in a manner that affirms democratic values."

[1] https://www.w3.org/TR/vc-data-model/
[2] https://www.w3.org/TR/did-core/
[3] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf

It states that "… there are no widely adopted standards for data formats, application programming interfaces, or system architectures that are necessary to facilitate the interoperability and deployment of PPDSA technologies." Accordingly, the Strategy calls for the federal government to "strategically engage with academia, the private sector, and standards development organizations to study and develop standards for PPDSA technologies."

In addition, the Strategy provides the following recommendations to accelerate translation to practice:

- "Federal funding opportunities and programs that support translational projects and early-stage startups should be expanded with a focus on PPDSA technologies to close the gap between theory and practice."
- "Federal agencies should explore and identify opportunities to pilot PPDSA technologies and pursue new forms of data collaboration[.] Pilot programs should include plans for how the PPDSA technologies will be transitioned for a successful deployment."
- "The Federal Government should explore opportunities to fund open-source efforts in support of the PPDSA ecosystem."

By working at the intersection of DHS operational needs and existing DHS investments in W3C VCDM and W3C DID standards, **whose data formats, application programming interfaces (APIs) and system architectures can enable PPDSA technologies that facilitate global interoperability in the issuance and verification of digital credentials**, and combining that with SVIP's demonstrated ability to find and work with innovative, global startup talent and technologies to meet DHS operational needs, this SVIP Call seeks to:

- catalyze, develop, enhance, and operationalize a set of privacy preserving building blocks that can support the needs of a privacy preserving digital credentialing ecosystem; and
- ensure that solutions support and enable an ecosystem that is accessible, open, competitive, diverse, and vibrant.

1.3. Illustrative Scenarios

The following illustrative scenarios are intended to describe where the technologies being sought by DHS in this Topic Call could potentially be applied. **DHS is not necessarily seeking the technologies for these specific scenarios but instead is providing them to give some context for interested parties.**

The scenarios highlight the future being envisioned and being built across multiple local and global jurisdictions and stakeholders to enable, encourage, and support a plurality of **independent, interoperable, standards-based implementations.**

Such implementations counter vendor/technology lock-in, and mitigate perverse incentives that accrue market power to entities that can result in a gatekeeper functionality between the Government and its customers, while:

- supporting an individual's desire for agency and control in their digital interactions;
- minimizing the disclosure of personal data via implementing informed consent management and selective disclosure capabilities;
    - Selective disclosure within this context means that a digital credential could hold many individual pieces of information that could meet the variety of needs of both government and non-government entities, while all information is not needed for

each encounter. So, the ability to selectively share, with consent, just the pieces of information that are needed for a particular encounter is a highly desired capability.
    - Some potential examples of this could be that a person, after going through the immigration process and obtaining credentials, upon re-entry, may be required to share with the government just enough information to prove that they are authorized for re-entry or a credential holder seeking to purchase items for which they must be a certain age having the ability to disclose just enough information that allows them to prove that they meet those criteria.
- supporting both online and in-person presentation and verification of credentials; and
- enabling protected, secure data processing and end-to-end platform attestations as an alternative that could, in the long term, minimize the use of biometric matching technologies for identity verification in the credentialing ecosystem.

Because responses to this OTS Call may be relevant to these and other scenarios, it is expected that an applicant will use one or more of these stakeholder scenarios to frame their application.

1.3.1. Scenario I: DHS Issuing Credentials to a Digital Wallet Holder

USCIS administers the nation's lawful immigration system and is responsible for the issuance of documentary evidence of citizenship, immigration, and employment authorization.

The application of technologies sought in this Topic Call could potentially enhance USCIS capabilities to:

- Issue digital immigration credentials to a CBP Mobile Digital Wallet e.g., CBP One Mobile Application, to meet the needs of the Western Hemisphere Travel Initiative (WHTI);
- Issue digital immigration credentials to State Partner Government Digital Wallets e.g., California DMV Open-Source Digital Wallet, for use by their residents in online and in-person interactions;
- Issue digital immigration credentials to Digital Wallets assessed and approved by our International Partner Governments e.g., Government of Canada, the European Union Member States etc., such that the holder can assert U.S. immigration status, residency, and employment eligibility with both public and private sector verifiers; and/or
- Issue digital immigration credentials to Digital Wallets that meet DHS requirements for security, privacy, and interoperability, such that the holder can assert U.S. immigration status, residency, and employment eligibility with both public and private sector verifiers.

CBP, as the United States' first unified border entity, takes a comprehensive approach to border management and control, combining customs, immigration, border security, and agricultural protection into one coordinated and supportive activity.

The application of technologies sought in this Topic Call could potentially enhance CBP capabilities to:

- Issue W3C VCDM/DID credentials, for which it is authoritative, into Digital Wallets.

1.3.2. Scenario II: Digital Wallet Holder sharing information with a DHS Verifier

CBP, as the United States' first unified border entity, takes a comprehensive approach to border management and control, combining customs, immigration, border security, and agricultural protection into one coordinated and supportive activity.

The application of technologies sought in this Topic Call could potentially enhance CBP capabilities to:

- Verify W3C VCDM/DID credentials at web, kiosk, mobile and in-person infrastructure, stored in a CBP Mobile Digital Wallet e.g., CBP One Mobile Application, to facilitate entry into the United States for U.S. citizens and legitimate international travelers, making the process more efficient and convenient while supporting the WHTI;
- Verify W3C VCDM/DID credentials at web, kiosk, mobile and in-person infrastructure, stored in State Partner Government Digital Wallets e.g., California DMV Open-Source Digital Wallet, to facilitate entry into the United States for U.S. citizens and legitimate international travelers, making the process more efficient and convenient while supporting the WHTI;
- Verify W3C VCDM/DID credentials at web, kiosk, mobile and in-person infrastructure, stored in Digital Wallets assessed and approved by our International Partner Governments e.g., Government of Canada, the European Union Member States etc., to facilitate entry into the United States for legitimate international travelers, making the process more efficient and convenient while supporting the WHTI; and/or
- Verify W3C VCDM/DID credentials at web, kiosk, mobile and in-person infrastructure, stored in Digital Wallets that meet DHS requirements for security, privacy, and interoperability, to facilitate entry into the United States for legitimate international travelers, making the process more efficient and convenient while supporting the WHTI.

USCIS administers the nation's lawful immigration system and is responsible for the issuance of documentary evidence of citizenship, immigration, and employment authorization.

The application of technologies sought in this Topic Call could potentially enhance USCIS capabilities to:

- Verify W3C VCDM/DID credentials and other authoritative documentation at web, kiosk, mobile and in-person infrastructure, stored in a CBP Mobile Digital Wallet e.g., CBP One Mobile Application, that are required for immigration benefits adjudication;
- Verify W3C VCDM/DID credentials and other authoritative documentation at web, kiosk, mobile and in-person infrastructure, stored in State Partner Government Digital Wallets e.g., California DMV Open-Source Digital Wallet, that are required for immigration benefits adjudication;
- Verify W3C VCDM/DID credentials and other authoritative documentation at web, kiosk and in-person infrastructure, stored in Digital Wallets assessed and approved by our International Partner Governments e.g., Government of Canada, the European Union Member States etc., that are required for immigration benefits adjudication; and/or
- Verify W3C VCDM/DID credentials and other authoritative documentation at web, kiosk and in-person infrastructure, stored in Digital Wallets that meet DHS requirements for security, privacy, and interoperability, that are required for immigration benefits adjudication.

1.3.3. Scenario III: Digital Wallet Holder sharing information with a non-DHS Verifier

High value credentials issued by CBP and USCIS are used across both the public and private sector for a variety of purposes including asserting residency and employment eligibility and for Know Your Customer (KYC). In addition, as Digital Wallets become widely used, a U.S. Person may need a Digital Wallet for travel to a jurisdiction where they are required for certain online and in-person interactions.

The application of technologies sought in this Topic Call could potentially enhance non-DHS entity capabilities to:

- Verify DHS issued W3C VCDM/DID credentials and other authoritative documentation at web, kiosk, mobile and in-person infrastructure, stored in a CBP Mobile Digital Wallet e.g., CBP One Mobile Application, in support of relevant online and in-person interactions;
- Verify DHS issued W3C VCDM/DID credentials and other authoritative documentation at web, kiosk, mobile and in-person infrastructure, stored in State Partner Government Digital Wallets e.g., California DMV Open-Source Digital Wallet, in support of relevant online and in-person interactions;
- Verify DHS issued W3C VCDM/DID credentials and other authoritative documentation at web, kiosk and in-person infrastructure, stored in Digital Wallets assessed and approved by our International Partner Governments e.g., Government of Canada, the European Union Member States etc., in support of relevant online and in-person interactions; and/or
- Verify DHS issued W3C VCDM/DID credentials and other authoritative documentation at web, kiosk and in-person infrastructure, stored in Digital Wallets that meet DHS requirements for security, privacy, and interoperability, in support of relevant online and in-person interactions.

2. Topic Description

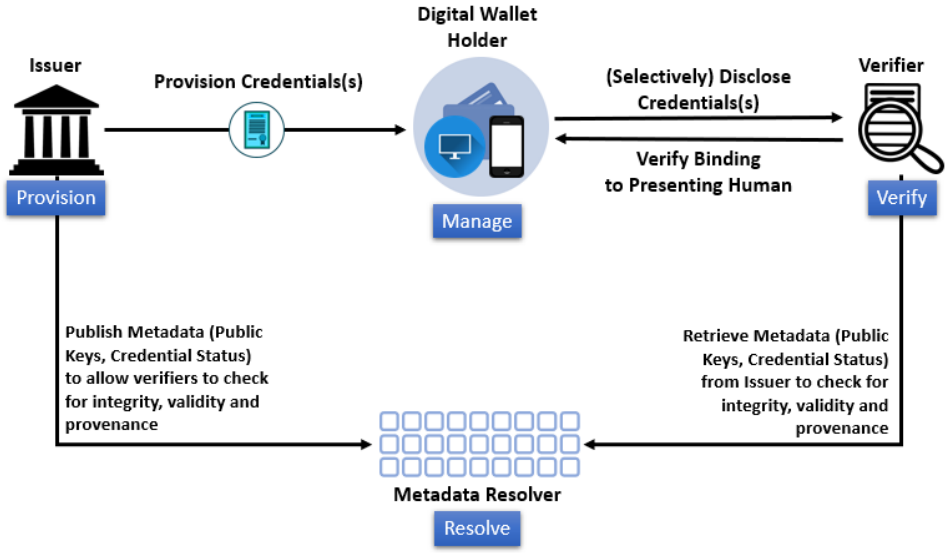
2.1 Topic Call Conventions

The International Organization for Standardization (ISO) uses specific verbal forms to convey clarity on what is a requirement and what is a recommendation or other type of statement. This Topic Call adopts and uses the following ISO document conventions:

- Requirements - SHALL, SHALL NOT
- Recommendations - SHOULD, SHOULD NOT
- Permission - MAY, MAY NOT
- Possibility and Capability - CAN, CANNOT

2.2 Assumptions and Constraints

Applicants are assumed to know the concepts and terms presented in W3C VCDM and W3C DID global standards.



NOTE: The W3C VCDM Standard identifies an abstract component called a "Verifiable Data Registry" which in DHS implementations is referred to as a "Metadata (or Public Key) Resolver"

DHS implementation of digital credentials using the W3C VCDM and W3C DID standards have the following principles that we consider critical in meeting the expectations and needs of our global customer base, that must be part of any proposed solution:

- Support for selective disclosure capabilities to provide the holder of the credential granular control over what information they can share and when;
- Elimination of "phone home" architectures, technologies, and implementations;
- Elimination of "back-channel" interactions between verifiers of the credentials and the issuers which are not visible to the credential holder; and
- Support for open, standards-based digital wallets that do not require a Memorandum of Understanding (MOU)/business relationship with the wallet vendor or require the use of proprietary digital wallet APIs.

Proposed solutions and implementations SHALL be limited to those that support the W3C VCDM Credential Data Model Representation Syntax and W3C VCDM Credential Data Model Proof Formats required by the "DHS Implementation Profile of W3C VCDM and W3C DID" utilized by USCIS and CBP (Relevant portions provided below):

Credential Data Model Representation Syntax

- Verifiable Credentials and Verifiable Presentations, as defined in W3C VCDM, SHALL be serialized as W3C JSON-LD[4] in compacted document form
    - A Verifiable Credential SHALL define all terms using @context
    - A Verifiable Presentation SHALL define all terms using @context

[4] https://www.w3.org/TR/json-ld11/#compacted-document-form

  - W3C JSON-LD SHALL define all types using @type
  - W3C JSON-LD SHOULD leverage objects instead of strings to refer to Issuers and Holders
  - W3C JSON-LD MAY rely on @vocab to automatically define terminology

Credential Data Model Proof Format

- Verifiable Credentials, as defined in W3C VCDM, SHALL be secured using the Data Integrity Proof format
  - Data Integrity Proof format SHALL implement mandatory U.S. Federal Information Processing Standards (FIPS) Compliant Cryptography
  - Data Integrity Proof format SHALL implement interoperable security engineering best practices
  - Data Integrity Proof format SHALL implement interoperable privacy engineering best practices
- Verifiable Credentials, as defined in W3C VCDM, MAY be secured using the JSON Web Token Proof format
  - JSON Web Token Proof format SHALL implement mandatory U.S. FIPS Compliant Cryptography
  - JSON Web Token Proof format SHALL implement interoperable security engineering best practices
  - JSON Web Token Proof format SHALL implement interoperable privacy engineering best practices

Providing Credential Provisioning and Credential Presentation APIs that are publicly documented, patent free, royalty free, non-discriminatory, and available to all mitigates technology and vendor risk to Issuers, Holders and Verifiers while simultaneously providing technology providers the ability to build innovative and value-added solutions behind the API.

To that end, the following are specific items to be incorporated into each Technical Topic Area (TTA) listed below to ensure that solutions are secure, privacy respecting, scalable and interoperable:

- All Holder APIs SHALL be publicly documented, patent free, royalty free, non-discriminatory, available to all, and free to implement using widely available and supported programming languages.
- The solution SHALL support FIPS compliant cryptographic algorithms for hashing, encryption, digital signatures, random number generation and any other relevant cryptographic operations that are performed as part of the solution to ensure its ability to be operationally deployable on a U.S. Government network.
- The Holder SHALL have the ability to choose and utilize (register, select, use) one or more digital wallets that meet openly defined and testable security, privacy and interoperability considerations of Issuers and Verifiers to store and present credentials.
- The solution SHALL incorporate, at a minimum and as appropriate to the scenario and TTA, the following emerging standards and/or specifications for interoperability that have been funded, tested and/or deemed relevant to DHS:
  - DID Resolution[5] (W3C) for Metadata Retrieval
  - Status List 2021[6] (W3C) for Privacy Enabled Revocation Checks

[5] https://w3c-ccg.github.io/did-resolution/
[6] https://w3c.github.io/vc-status-list-2021/

  - did:web Method Specification[7] (W3C) for Organizational Identity
  - The BBS Signature Scheme[8] (IETF) for Selective Disclosure with Unlinkability
- The solution MAY incorporate, as appropriate to the scenario and TTA, the following additional standards and/or specifications in a manner that SHALL meet the desired Digital Wallet Selection capability as well as the Credential Data Model Representation Syntax and Credential Data Model Proof Formats required by the "DHS Implementation Profile of W3C VCDM and W3C DID" specified earlier in this document:
  - Verifiable Credentials API[9] (W3C) for Provisioning and Presentation
  - Credential Handler API[10] (W3C) for Digital Wallet Selection
  - OpenID for Verifiable Credential Issuance
  - OpenID for Verifiable Presentations
  - Selective Disclosure for JWTs (SD-JWT)[11]
  - Remote Attestation Procedures[12] (IETF)
  - Apple iOS App Attest[13]
  - Google Android Play Integrity[14]

NOTE: Existing investments by DHS in the W3C VCDM and W3C DID standards and implementations have resulted in a global, vibrant, multi-vendor ecosystem that addresses the need for market choice and can support multi-vendor interoperability while mitigating vendor and platform lock-in concerns.

It is expected that any company awarded an Other Transaction Agreement (OTA) under this Call will actively participate in and support, as relevant to their implementation, any emerging specifications and standards that ensure multi-platform, multi-vendor interoperability to ensure they mature to become open, global, royalty and patent free and free to implement standards.

[7] https://w3c-ccg.github.io/did-method-web/
[8] https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-signatures/
[9] https://w3c-ccg.github.io/vc-api/
[10] https://w3c-ccg.github.io/credential-handler-api/
[11] https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/
[12] https://datatracker.ietf.org/wg/rats/about/
[13] https://developer.apple.com/documentation/devicecheck/establishing_your_app_s_integrity
[14] https://developer.android.com/google/play/integrity

3. Technical Topic Areas (TTAs)

Program Intent
DHS is seeking technologies and solutions that address its need via one or more of the following TTAs. While DHS is interested in meeting the goals of all the TTAs, DHS wants to make it clear that doing so is not a requirement and as such **you are encouraged to apply even if your prototype project meets only one TTA.** However, to ensure broad adoption and deployment of the privacy preserving technologies and solutions that are sought in this Topic Call, DHS requires that TTAs incorporate foundational modules that are implemented as stand-alone, open-source software libraries (OSLs) provided as Software Development Kits (SDKs) that have the following properties: • Comprehensive documentation at the library and at the code level; • Test suites/artifacts to test and verify the libraries; and • Uses an open-source license that ensures that the software library is patent free, royalty free, non-discriminatory, available to all and free to implement and utilize in both open source and closed source products on a global basis. e.g., Apache License 2.0 etc. **Responses from offerors SHALL be any one or a combination of TTAs** • **Each TTA SHALL include one or more OSLs from Section 3.3**

3.1. TTA #1: Digital Wallet

The digital wallet under the control of an individual can have many aspects including hardware, secure storage and processing of sensitive information, and cryptographic operations performed remotely or locally and implemented as portable hardware devices, secure web applications, native mobile applications, plug-ins to browsers, extensions to cross-platform password/credential managers, and more.

DHS is seeking digital wallets that are useful across contexts and jurisdictions, can support the broad range of credentials possible with W3C VCDM/DID standards that include verified support for DHS issued credentials, and is "portable, highly secure, privacy-preserving, standards-based, interoperable and multi-function"[15] as described by the Linux Foundation's "Open Wallet Foundation (OWF)" initiative.

Using the OWF terminology as a reference, DHS is specifically interested in wallets that support "identity" functions and is neutral regarding the capabilities that the wallet may have as regards to "payment" and "access" functions; provided those additional functions do not compromise the security, privacy and interoperability required by our implementation profile.

The solutions being sought enable the following outcomes:

- Support multiple issuers and verifiers using open, standardized APIs

[15] https://project.linuxfoundation.org/hubfs/LF%20Research/OpenWallet%20Open%20Digital%20Wallet%20-%20Report.pdf?hsLang=en

- Support for provisioning, revocation, and re-issuance of cryptographic material and credentials stored within the digital wallet.
- Intuitive user interface implementations that provide a high degree of usability to a non-technical audience
- Support for multiple languages in the user interface

Analysis and recommendations that support and articulate the trade-offs associated with implementation choices are an important aspect of the information sought as part of any proposed solution.

Implementations of this capability SHALL incorporate one or more OSLs from Section 3.3

3.2. TTA #2: Mobile Verifier

Verifiers are entities that validate credentials presented to them and ensure that the asserted information is bound to the individual presenting the credential(s).

DHS is seeking software-based Verifier implementations that can be deployed on mobile devices, including on iOS and Android based devices, that can support the broad range of credentials possible with W3C VCDM/DID standards to include verified support for DHS issued credentials.

The solutions being sought enable the following outcomes:

- Support for the dynamic retrieval of public keys, and the ability to cache them locally for a length of time that is determined by policy; from issuers using the resolution mechanism enabled by the W3C DID standard with explicit support for the did:web method for organizational identities
- Support for cryptographically validating the integrity of credentials using signature methods that are FIPS compliant, as well as other signature methods that enable selective disclosure mechanisms as shared in the “Assumptions and Constraints” section of this Call.
- Support for checking the revocation status of the credentials using approaches that do not support a “phone home” approach as shared in the “Assumptions and Constraints” section of this Call.
- Support for notifying the Holder of the Verifier’s authorized purpose and use of data shared with it.

Analysis and recommendations that support and articulate the trade-offs associated with implementation choices are an important aspect of the information sought as part of any proposed solution.

Implementations of this capability SHALL incorporate one or more OSLs from Section 3.3

3.3. Open-Source Libraries (OSLs)

OSL (A): Cryptographic Tools SDK for Issuers, Digital Wallets, and Verifiers

This SDK, when implemented by an issuer, a digital wallet or a verifier makes available to it a suite of cryptographic tools to enable hashing, signing, bulk encryption, streaming encryption, random number generation and more, that can support FIPS compliant cryptography, selective disclosure capabilities, and other privacy preserving cryptographic schemes.

Analysis and recommendations in how this SDK can support cryptographic agility and layering with a path to quantum safe cryptography is an important consideration.

It is expected that this module will be developed in a manner that will enable assessment by the Cryptographic Module Validation Program (CMVP), which is a joint effort between the National Institute of Standards and Technology under the U.S. Department of Commerce and the Canadian Centre for Cyber Security, a branch of the Government of Canada's Communications Security Establishment. The goal of the CMVP is to promote the use of validated cryptographic modules and provide Federal agencies with a security metric to use in procuring equipment containing validated cryptographic modules.

OSL (B): Sealed Storage SDK for Issuers, Digital Wallets, and Verifiers

This SDK, when implemented by an issuer, a digital wallet or a verifier makes available to it storage capabilities where data can be locked until specific software and/or hardware conditions are met. This capability supports the secure and protected storage of data such as cryptographic keys and other sensitive information.

Analysis and recommendations in how this SDK could support both local and remote storage capabilities as well as austere or occasionally connected networks are important considerations.

OSL (C): Metadata Management SDK for Issuers, Digital Wallets, and Verifiers

This SDK, when implemented by an issuer, a digital wallet or a verifier makes available to it capabilities that allow it to retrieve metadata associated with credential issuance and verification and cache it locally as allowed by configurable policy. The metadata will include, at a minimum, the following:

- Retrieval and validation of DID documents using W3C DID resolution APIs
- Credential status information provided via W3C VC Status List

OSL (D): Confidentiality and Integrity Protected Computing SDK for Issuers, Digital Wallets, and Verifiers

This SDK, when implemented by an issuer, a digital wallet or a verifier makes available to it capabilities that allow it to utilize confidential computing capabilities that protect data in use by performing computations in a hardware-based, attested Trusted Execution Environment and to generate and consume attestations that are necessary to evaluate its operations.

It is anticipated that these capabilities will be particularly relevant to the three-party digital identity model in the areas of cryptographic key management and operations.

Analysis and recommendations in how this SDK could support both local and remote attestations as well as austere or occasionally connected networks are important considerations.

4. Project Deliverables and Phases

The SVIP is generally structured in 4 Phases, with an opportunity to award a Phase 5 for further testing/piloting in additional operational environments and potentially addressing additional use cases. For the purposes of this project, all applicants shall submit a Phase 1 application.

SVIP Phase detail is listed in the following chart:

Phase	Funding Level & Source	Deliverables	Due Date
1	**$50,000 to $200,000**	**Minimum Viable Product demonstrating proof-of-concept of adaptation**	**6–9 months after award**
2	$50,000 to $500,000	Prototype development building out all features to demonstrate viability	6–9 months after successful completion of Phase 1
3	$50,000 to $500,000	Prototype deployed in realistic test and evaluation (T&E) environment for independent T&E and red teaming	6–9 months after successful completion of Phase 2
4	$50,000 to $500,000	Operational testing of developed capability fully coordinated with DHS Component and operational stakeholders	6-9 months after successful completion of Phase 3
5	TBD at the Government's discretion	Additional operational testing which may include additional use cases in additional operational environments	Begin after successful completion of Phase 4

Referring to the table above, the required milestones and deliverables for each Phase shall incorporate the objectives defined as follows:

- **Phase 1:** Delivery of a Minimum Viable Product that demonstrates proof-of-concept and supporting documentation inclusive of verifiable test evidence, technical drawings, and software demonstrations or other proof that the technical approach to address a DHS requirement or challenge as identified in this Call is sound. At the end of this Phase, successful applicants will have:

- Created a proof of concept of a new technology suitable for demonstration, or
- Produced reviewable modifications to pre-existing technologies suitable for demonstration, or
- Documented a go-to-market commercialization strategy that includes any information that is relevant to how the solutions address equity and access for underserved populations and communities.
- Community contribution report regarding the development of the OSLs

- **Phase 2**: An end-to-end working prototype with full capabilities. Objectives of this phase are to use the results of Phase 1 to build out all features and functions in the prototype to demonstrate viability. At the end of Phase 2, the prototype must:
  - Demonstrate end-to-end operational viability
  - Be ready for independent review and evaluation
  - Validate the commercialization strategy with potential customers and partners
  - Community contribution report regarding the development of the OSLs
- **Phase 3**: A production ready prototype that will be deployed into a realistic T&E environment to experiment against realistic conditions and undergo an independent T&E process to ensure operational suitability. These tests will be fully coordinated with the DHS Component and relevant operational and oversight stakeholders, and it is anticipated that all independent testing feedback will be incorporated into the technology solution by the end of this Phase. Objectives of this phase are to:
  - Demonstrate a fully functional end to end capability
  - Support the functional, security, privacy, and interoperability testing and validation of the capability by an independent Red Team

Program Intent
Red Team testing in this phase will include an in-depth, independent code review of the OSLs; DHS will broadly socialize and seek feedback on the results of the code reviews.

  - Incorporate the feedback and results of the independent test into the prototype
  - Community contribution report regarding the development of the OSLs
- **Phase 4**: Delivery of technologies with fully completed designs and which reputably provide all proposed features and functionality. Any tests and demonstrations in this Phase will be fully coordinated with the DHS Component and relevant operational and oversight stakeholders and may result in a limited number of prototypes or licenses of the technology to conduct the testing in multiple user scenarios and conditions. Objectives of this phase are to:
  - Deploy the capability for operational testing and demonstration

Program Intent
The operational testing and demonstrations may include interoperability testing and plug-fests with International Government Partners e.g., Government of Canada, the EU/EC and others, who are developing and deploying similar capabilities in order to ensure global interoperability across jurisdictions.

  - Incorporate and adjust the capability based on the operational testing
  - Community contribution report regarding the development of the OSLs

- **Phase 5**: Phase 5 awards are made only to meet a Government need and additional testing requirements. The additional testing may be done in different environments using additional use cases. This Phase may result in a limited number of prototypes or licenses of the technology to test the prototype in multiple user scenarios and conditions. To meet an identified Government need, this phase may be funded beyond the total Phases 1-4 limits.

The Government may choose to combine and/or skip later Phases, which will be determined after the successful completion of the Phase 1 effort and subject to the Government's invitation. See 5-Year Innovation OTS (70RSAT21R00000006) Section 2.2.3.

For the purposes of this project, DHS S&T anticipates making Phase 1 awards of $50,000 to $200,000 in funding for each award, with an estimated period of performance of 6 to 9 months. Successful projects will be eligible for subsequent phases of funding with a ceiling range between $50,000-$500,000 per phase (or in total $200,000-$1,700,000 for Phases 1-4) and duration to be approximately six (6) to nine (9) months per Phase. The ceilings of the subsequent Phases are based on multiple factors such as DHS needs and available funds. DHS will provide the specific Phases 2-4 ceiling amounts for this Topic Call during the Phases 2- 4 invitation process. See 5-Year Innovation OTS (70RSAT21R00000006) Section 2.2.1.

A Phase 5 may be awarded if the Government determines that further operational testing is required, and/or the technology is applicable in additional DHS use cases. Phase 5 OTAs will be scaled to fit the mission need/requirement in both cost and length of time and are not restricted by the Phases 1-4 ceilings listed above.

Project Phase awards are dependent on progress made by the applicant, DHS needs, and availability of funds. To receive consideration for subsequent Phases, applicants shall be invited by the Government to submit an application for each Phase. The Government reserves the right to not make subsequent Phase awards.

Phase 1 shall not exceed $200,000, and Phases 2-4 shall not exceed $500,000 per Phase for a total of $1,700,000.

At the end of Phase 4, DHS S&T intends that successful projects shall have reached a sufficient stage of development to be production-ready for deployment or commercial availability to stakeholders, including a potential follow-on production contract or OTA by DHS.

The specific phased approach set out above is general program guidance and not a mandatory structure. At the sole discretion of the Government, each OTA project award may begin at any Phase, or make use of combined or skipped Phases, in order to accommodate different technology and different maturity levels of an awardee's products. Any variations, such as combining Phases and/or skipping Phases, may be made based on technical maturity of the solutions received.

5. General Information and Instructions

5.1 Response Dates

We encourage you to submit your applications well before the deadline!

Event	Time Due	Date or Date Due
Industry Day Register to attend at: https://sri-csl.regfox.com/svip-digital-wallet-industry-day	N/A	Please see the registration link for Industry Day date, time and location.
Applications Due Date: Applications will be accepted on a continuous, rolling basis until the application deadline. The deadline for submitting an application is listed on the right. **Applications shall be received prior to the deadline to be evaluated in the review cycle.**	12:00 PM (Noon) PT / 3:00 PM ET*	September 15, 2023
Notification of Application Pre-Oral Pitch Evaluation Results	N/A	Approximately 45 days following the application deadline
Oral Pitches	N/A	Approximately 60 days following the application deadline (if requested)
Closing Date/Final Deadline	September 15, 2023 12:00 PM (noon) PT / 3:00 PM ET*	

* Eastern Time (ET), Pacific Time (PT)

Applications and application resubmissions shall be submitted by the due dates listed above to be reviewed in that cycle. DHS will conduct reviews following each submission deadline and anticipates that reviews will be completed within approximately 45 days following each submission deadline.

Under no circumstances will applications and application resubmissions received after the Final Deadline date and time be considered for review.

DHS may decide to close the Call early. If this occurs, DHS will publish a notification on SAM.gov 30 days prior to closing the Call.

Applicants shall check SAM.gov for any amendments and changes to this Topic Call.

5.2 Eligibility

Applicants **SHALL** determine if they are eligible to apply to this solicitation by reviewing the SVIP OTS 70RSAT21R00000006 section 4 and the eligibility section of the FAQ document posted with the Topic Call. Any applications received from ineligible applicants will be rejected.

5.3 General Instructions

5.3.1 Any invitations for oral pitches will be coordinated with the applicant and will be conducted via a virtual online meeting platform (e.g., MS Teams).

5.3.2 The Government may request applications for other Phases and will do so directly with the company.

5.3.3 DHS S&T reserves the right to fund all, some, parts, or none of the applications received in response to this Topic Call.

5.4 Application Format, Instructions and Requirements

Applicants shall register in the OIP/SVIP Web Portal and complete all requested company information, upload the Technical Volume and Cost/Schedule Volume (TV & CSV) and Section 889 Provisions and Clauses document as PDFs prior to the final closing date and time. Applications are no longer being accepted by email.

Web Portal: The applicant shall register for an account, complete company information, apply to the Topic Call, upload the TV, CSV, and Section 889 Provisions and Clauses document and finalize their application submission.

Technical Volume (TV): The applicant shall provide technical details associated with the proposed work. This document shall not exceed 8 pages and shall be uploaded to the web portal when applying to the Topic Call.

Cost/Schedule Volume (CSV): The CSV spreadsheet has 5 tabs. The first four tabs are cost-related and the 5th tab contains the schedule chart.

Section 889 Provisions and Clauses: Section 889 of the FY 2019 National Defense Authorization Act (NDAA) contains prohibitions related to certain covered telecommunications equipment or services. Section 889 defines "covered telecommunications equipment or services" as telecommunications and video surveillance equipment or services produced by Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company, or any subsidiary or affiliate of such companies. Please check the appropriate box highlighted in yellow on pages 2, 7, and 8 of the Section 889 Provisions and Clauses document and upload the completed document to the web portal.

Application: This is the final document that includes all of the information entered into the web portal and in the TV, CSV, and Section 889 Provisions and Clauses document once the submission process is complete, DHS will review the documents.

After applicants have confirmed their eligibility, applicants **SHALL** do the following:

Step 1: Register for an account through the OIP/SVIP Web Portal
Please see the "Public Portal Registration Guide" posted with this Topic Call**.** Please note you will need your company Tax Identification Number (TIN) for this step. If you don't have a TIN, instructions for receiving a temporary number are provided on the website**. Please note that a unique entity identification number (UEID) is not required for this step but is highly recommended. To register for a UEID, please go to SAM.gov and register your entity for "All Awards".**

Step 2: Apply to the Privacy Preserving Digital Credential Wallets & Verifiers Topic Call through the OIP/SVIP Web Portal, proceed through each tab, answering all questions and complete the requested information.

- **Apply by the deadline of September 15, 2023 12:00 PM PT/3:00 PM ET.** Please select "PPDC". Please note that the Portal will shut down right after the closing date and time even if you are still in the process of applying, so **DO NOT** wait until the last minute to submit.

Step 3: Under the Supporting Documents tab, complete the Privacy Preserving Digital Credential Wallets & Verifiers TV, CSV (separate spreadsheet template with 5 tabs), and Section 889 Provisions and Clauses document and upload to the OIP/SVIP Web Portal.

Technical Volume:

- The TV shall not exceed 8 pages and shall be one pdf file. Any other format will not be accepted.
- At least one TTA shall be selected in the TV (see the check boxes in section 1.1 in the TV template). If the proposed technology addresses multiple TTAs, check the applicable TTAs. Applicants shall not submit a separate TV for each TTA; applicants shall address all applicable TTAs in one TV.
    - All Sections of the application (both in the web portal and TV) shall be completed. This includes sections with "Yes" and "No" boxes; applicants shall check one of the boxes.
    - The TV, including the Architectural/Intellectual Property diagram, shall not exceed 8 pages.
    - The TV shall describe the work proposed for Phase 1 and all questions shall be answered.
    - Only content contained in the final application will be considered during the review process. No other documents, videos or links to information will be considered.

Cost and Schedule Volume:

- The Phase 1 amount shall not exceed $200,000.
- Save each individual tab of the CSV as separate PDFs and upload each to the portal (total of 5 PDFs)

- **Section 889 Provisions and Clauses:** Please check the appropriate boxes highlighted in yellow on pages 2, 7, and 8 of the Section 889 Provisions and Clauses document and upload the completed document to the web portal.

Total Application submission: One Technical Volume PDF file, five Cost and Schedule Volume

PDF files, and one Section 889 Provisions and Clauses document for a total of 7 uploaded documents.

Step 4: Complete your application submission via the OIP/SVIP Web Portal

- Review and click the Submit button
- Applicants will receive a confirmation email once their application is successfully submitted.
    - Applications shall be compliant with the aforementioned response due date and other compliance requirements in accordance with the DHS S&T SVIP 5-Year Innovation OTS (70RSAT21R00000006). **Submissions not in compliance shall be rejected.**

Applicants shall apply to the Topic Call using the portal as noted in the steps above. Please contact the portal helpdesk if you encounter any technical issues.

Monday - Friday
9:00 am - 5:00 pm ET
(571) 446-4869
OIPPortalHelpDesk@hq.dhs.gov

5.5 Evaluation Criteria

The OTS evaluation criteria published in the DHS S&T SVIP Other Transaction Solicitation 70RSAT21R00000006 will be utilized for the application evaluation process, and specific to this Call, applications will be reviewed for:

Criterion I: **Responsiveness to Technical Topic and Technical Approach**. The potential of the technology/solution to meet the project TTA goals provided in the OTS Call will be assessed, along with the technical and managerial approach to the proposed work.

- Applicability to the DHS illustrative use case(s) or other credible use case(s), including how well the proposed technology/solution promotes privacy requirements and best practices.
- Incorporation of the DHS assumptions and constraints in the solution being proposed
- Sufficient technical evidence that the solution will address the problem stated.

Criterion II: **Applicant's Capabilities and Related Experience**. The applicant's prior experience in similar efforts will be assessed to determine if the applicant clearly demonstrates an ability to deliver products that meet the proposed technical performance. The assessment for this criterion will include evaluating the experience of key personnel and any corporate viability requirements specified in the Topic Call.

- Financial soundness of the company, and the business model based on the technology to be supported.

Criterion III: **Transition Approach**. A qualitative assessment will be made regarding how the proposed technology/solution will be transitioned to an operational user (e.g., commercialized or used by a DHS Component). The assessment will determine the likelihood that the applicant will be able to deploy a technology and/or solution(s) that can be transitioned effectively to the user community.

- The scalability and cost-effectiveness of the proposed technology or solution;

- Existing relationships with relevant end users, stakeholders and/or consumers;
- Ability to help DHS operational missions or critical infrastructure facilities.

5.6. Pitch Format and Requirements

Applicants invited to present pitches will be limited to fifteen (15) minutes for their pitch. In addition, applicants making pitches may provide up to ten (10) slides for presentation in either Microsoft PowerPoint or Adobe PDF. Embedded videos demonstrating current product capabilities are encouraged.

Create a user account and register their company for "All Awards" in www.sam.gov

- This does not need to be done at the application phase but shall be done if the applicant is chosen to pitch and provides a successful pitch.

5.7 Contractual or Technical Inquiries

All contractual or technical inquiries to this OTS Call 70RSAT23R00000034 shall be emailed to DHS-Silicon-Valley@hq.dhs.gov. Emails submitting questions are to include **"Questions: Privacy Preserving Digital Credential Wallets and Verifiers Topic"** in the subject line. Questions will only be accepted and answered electronically.

5.8 Order of Precedence

In the event that any of the terms and conditions contained in this OTS Call 70RSAT23R00000034 conflict with terms and conditions included in SVIP 5 Year Innovation OTS (70RSAT21R00000006), the terms and conditions in this OTS Call 70RSAT23R00000034 shall take precedence.